T-79.5501 Cryptology
Exam
December 14, 2005

1. (6 pts) Let us consider a cryptosystem and the random variables related to it: plaintext $\mathbf{P}$, ciphertext $\mathbf{C}$ and key $\mathbf{K}$. As usual, $\mathbf{P}$ and $\mathbf{K}$ are assumed to be independent. Prove that then $\mathrm{H}(\mathbf{P}) \leq \mathrm{H}(\mathbf{C})$, and that $\mathrm{H}(\mathbf{P}) = \mathrm{H}(\mathbf{C})$ if and only if $\mathbf{C}$ and $\mathbf{K}$ are independent.

2. (6 pts) Find integers $x$ and $y$ such that $14x + 2005y = 12$.

3. Let us consider two binary linear feedback shift registers with connection polynomials $f(x) = x^4 + x^3 + x^2 + 1$ and $g(x) = x^3 + x^2 + 1$, where $g(x)$ is primitive.

   (a) (3 pts) Compute $\mathrm{lcm}(f(x), g(x))$.

   (b) (3 pts) Let $S_1$ be a sequence generated by the LFSR with polynomial $f(x)$ and $S_2$ be a sequence generated by the LFSR with polynomial $g(x)$. Determine the largest possible period of the sum sequence $S_1 + S_2$.

4. (a) (3 pts) Evaluate the Jacobi symbol

   $$\left(\frac{1223}{2005}\right).$$

   You should not do any factoring other than dividing out powers of 2.

   (b) (3 pts) Show that $2005 = 5 \cdot 401$ is an Euler pseudoprime to the base 1223.

5. Bob is using the *Rabin Cryptosystem*. Bob's modulus is $40741 = 131 \cdot 311$. Alice knows Bob's modulus but not its factors. Alice wants to remind Bob of an important date and sends it to Bob encrypted. The ciphertext is 38176.

   (a) (3 pts) Show how Bob decrypts the ciphertext. One of the possible plaintexts is a date, which Bob accepts and discards the other decryptions.

   (b) (3 pts) Alice happens to see one of the decryptions discarded by Bob. It is 20669. Show how Alice can now factor Bob's modulus.